

# Transmit Design for MIMO Wiretap Channel with a Malicious Jammer

Duo Zhang, Weidong Mei, Lingxiang Li, and Zhi Chen

National Key Laboratory of Science and Technology on Communications

University of Electronic Science and Technology of China, Chengdu 611731, China

Emails: zhangduo1st@gmail.com; mwduestc@gmail.com; walk22talk@gmail.com; chenzhi@uestc.edu.cn;

**Abstract**—In this paper, we consider the transmit design for multi-input multi-output (MIMO) wiretap channel including a malicious jammer. We first transform the system model into the traditional three-node wiretap channel by whitening the interference at the legitimate user. Additionally, the eavesdropper channel state information (ECSI) may be fully or statistically known, even unknown to the transmitter. Hence, some strategies are proposed in terms of different levels of ECSI available to the transmitter in our paper. For the case of unknown ECSI, a target rate for the legitimate user is first specified. And then an inverse water-filling algorithm is put forward to find the optimal power allocation for each information symbol, with a stepwise search being used to adjust the spatial dimension allocated to artificial noise (AN) such that the target rate is achievable. As for the case of statistical ECSI, several simulated channels are randomly generated according to the distribution of ECSI. We show that the ergodic secrecy capacity can be approximated as the average secrecy capacity of these simulated channels. Through maximizing this average secrecy capacity, we can obtain a feasible power and spatial dimension allocation scheme by using one dimension search. Finally, numerical results reveal the effectiveness and computational efficiency of our algorithms.

**Index Terms**—Physical-layer secrecy, artificial noise, power allocation, secrecy rate, malicious jammer, channel state information

## I. INTRODUCTION

Due to the broadcast nature of wireless medium, physical layer security approach is playing an increasingly important role in wireless communication recently. It can achieve significant security performance without using secret keys whose distribution and management may lead to security holes in wireless systems. Wyner's work in [1] has established the fundamentals of physical-layer secrecy since 1970's, in which the positive secrecy rate is proved to be achievable in a degraded wiretap channel; refer to [2] for a detailed overview of physical-layer secrecy. The past several decades have witnessed a rapid development of research on physical-layer secrecy, especially in the multi-input multi-output (MIMO) channels. For ease of exposition, we name the transmitter, the legitimate receiver and the eavesdropper *Alice*, *Bob* and *Eve*, respectively.

Different tactics against eavesdropper have been developed with various levels of eavesdropper channel state information

(ECSI) available to Alice. For the case of full ECSI, Khisti and Wornell extended Wyner's work to the multi-input, single-output, multi-eavesdropper (MISOME) and multi-input, multi-output, multi-eavesdropper (MIMOME) wiretap channel, respectively [3], [4]. Furthermore, some effective transmit designs are proposed to maximize the secrecy rate by adopting alternating optimization (AO) algorithm and generalized singular value decomposition (GSVD) algorithm in [5] and [6], respectively. For the case of unknown ECSI, Goel and Negi first proposed the technique of artificial noise (AN) to degrade Eve's channel [7]. While for the case of statistical ECSI, it is more intricate due to being less mature in comparison with that on full CSI and unknown CSI. Several works have focused on the statistical CSI recently. J. Li and A. P. Petropulu have proved the optimality of beamforming in the **MISOME** system where Eve's channel may have a nonzero mean or nontrivial covariance matrix [8], [9]. In [10], AN is taken into account in **MISOME** system, and the optimal power allocation strategy is determined by attaining the lower bound of the ergodic secrecy capacity. Moreover, an iterative algorithm is firstly proposed to deal with the **MIMOME** system with statistical ECSI in [11]. On the other hand, the impact of malicious jammer on the secrecy performance is another problem of long-standing interest. Seeking for the effective tactics against malicious jammer turns out urgent and critical in some special networks, such as, military networks. A prevalent approach is to model the transmitter and malicious jammer as players in a game-theoretic formulation [12]. Nevertheless, these game-theoretic-based works seldom concentrate on the optimal power allocation strategy for both parties. Actually, in order to degrade Eve's channel and guarantee Bob's reception quality simultaneously, the power allocation strategies turn out to be a dilemma. To the best of our knowledge, few studies work on the scenario for its challenges.

In this paper, we consider the transmit design for four-node multiple-antenna wiretap channel including a malicious jammer. We firstly show that the four-node wiretap channel can be transformed into the traditional three-node wiretap channel by whitening the interference at Bob. Based on the channel's transformation, different transmit schemes are proposed with various levels of ECSI available at Alice. Specifically, for the case of unknown ECSI, a novel optimization algorithm is put forward. A target rate for Bob is first set, and an inverse water-filling algorithm is derived to determine the optimal power

This work was supported in part by the Sichuan Province Science and technology program under Grant 2013GZ0029, and by the Important National Science and Technology Specific Projects of China under Grant 2014ZX03004003.

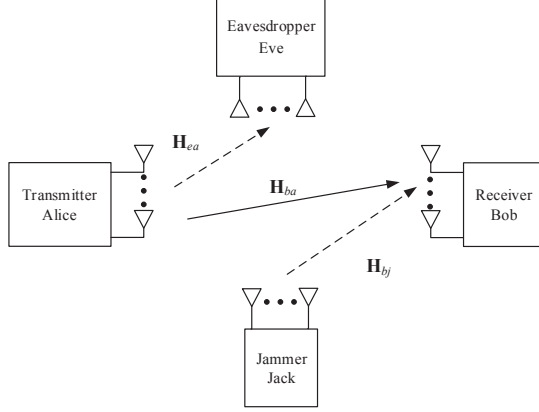


Fig. 1. MIMO wiretap channel with a malicious jammer

allocation scheme for Alice. Meanwhile, a stepwise search is then used to find the optimal spatial dimension allocated to AN such that the target rate is achievable. For the case of statistical ECSI, in view of the high computational complexity of the scheme proposed in [11], we simulate some random channel according to the distribution of ECSI. Then the ergodic secrecy capacity can be approximated as the average secrecy capacity of these simulated channels. To maximize the average secrecy capacity, we employ one dimension search to determine the optimal power allocation and optimal spatial dimension allocation between the information signal and AN. The numerical results verify the efficacy of our proposed schemes.

*Notation:* Bold symbols in capital letter and small letter denote matrices and vectors, respectively.  $(\bullet)^H$ ,  $\text{Tr}(\bullet)$ ,  $(\bullet)^{-1}$  and  $|\bullet|$  represent conjugate transpose, trace, inversion and determinant of a matrix.  $\mathbb{Z}_+$  is the set of nonnegative integers.  $\mathbf{I}$  denotes an identity matrix and  $[x]^+ = \max(0, x)$ .  $\mathbf{x} \sim \mathcal{CN}(\mu, \Omega)$  denotes that  $\mathbf{x}$  is a complex circular Gaussian random vector with mean  $\mu$  and covariance  $\Omega$ .  $\mathbf{A} \succeq \mathbf{0}$  implies that  $\mathbf{A}$  is a Hermitian positive semidefinite (PSD) matrix while  $\mathbf{x} \succeq \mathbf{0}$  implies that each component of  $\mathbf{x}$  is nonnegative.

## II. SYSTEM MODEL

Consider a four-node multiple-antenna wiretap channel including a malicious jammer, which is illustrated in Fig. 1. All terminals are equipped with multiple antennas. We will call the malicious jammer *Jack* for short. Suppose that Alice, Bob, Eve and Jack are equipped with  $N_A$ ,  $N_B$ ,  $N_E$  and  $N_J$  antennas, respectively. It is assumed that Jack only transmits AN to degrade Bob's reception and no information will be shared between Jack and Eve. The received signals at Bob and Eve can be modeled as

$$\mathbf{y}_b = \mathbf{H}_{ba}\mathbf{x}_a + \mathbf{H}_{bj}\mathbf{j} + \mathbf{n}_b \quad (1)$$

$$\mathbf{y}_e = \mathbf{H}_{ea}\mathbf{x}_a + \mathbf{n}_e \quad (2)$$

respectively, where  $\mathbf{H}_{ba} \in \mathbb{C}^{N_B \times N_A}$  and  $\mathbf{H}_{bj} \in \mathbb{C}^{N_B \times N_J}$  represent the MIMO channel from Alice and Jack to Bob, respectively, and  $\mathbf{H}_{ea} \in \mathbb{C}^{N_E \times N_A}$  represents the MIMO channel from Alice to Eve.  $\mathbf{x}_a \in \mathbb{C}^{N_A}$  is the signal transmitted by Alice.  $\mathbf{j} \in \mathbb{C}^{N_J}$  is the AN generated by Jack to jam Bob. Without loss of generality, the additive noise,  $\mathbf{n}_b \in \mathbb{C}^{N_B}$  and  $\mathbf{n}_e \in \mathbb{C}^{N_E}$ , are supposed as i.i.d. complex Gaussian noise with zero mean and unit variance. Since  $\mathbf{H}_{bj}$  is fixed over a sufficiently long period of time, Bob can detect it and then feed it back to Alice. It is reasonable to assume that  $\mathbf{H}_{ba}$  and  $\mathbf{H}_{bj}$  are both known to Alice, but  $\mathbf{H}_{ea}$  may be only fully or statistically known, even unknown to Alice.

Suppose that  $\mathbf{H}_{bj}$  is inaccessible to Jack, so it is an optimal strategy for Jack to transmit omni-directional AN [13], i.e.,

$$\mathbf{Q}_j = \frac{P_j}{N_j} \mathbf{I} \quad (3)$$

where  $\mathbf{Q}_j$  is the covariance matrix of  $\mathbf{j}$ ,  $P_j$  is the total transmission power of Jack.

In this paper, we focus on the optimization of the input covariance matrix design at Alice. The four-node-based secrecy rate maximization (SRM) design can be formulated as

$$\begin{aligned} R_s^* &= \max [R_b - R_e]^+ \\ \text{s.t. } &\text{Tr}(\mathbf{Q}_a) \leq P \end{aligned} \quad (4)$$

where  $R_b$  and  $R_e$  denote the achievable transmission rate between Alice and Bob/Eve, i.e.,

$$R_b = \ln \left| \mathbf{I} + (\mathbf{I} + \mathbf{H}_{bj}\mathbf{Q}_j\mathbf{H}_{bj}^H)^{-1} \mathbf{H}_{ba}\mathbf{Q}_a\mathbf{H}_{ba}^H \right| \quad (5)$$

$$R_e = \ln \left| \mathbf{I} + \mathbf{H}_{ea}\mathbf{Q}_a\mathbf{H}_{ea}^H \right| \quad (6)$$

in which  $\mathbf{Q}_a \triangleq E(\mathbf{x}_a\mathbf{x}_a^H)$  is the covariance matrix of  $\mathbf{x}_a$ .

Because the problem above is nonconvex, it's generally difficult to obtain the optimal solution. Note that when ECSI is unknown, this problem gets further intractable to deal with. To tackle it, we will simplify this problem by utilizing the interference whitening in the next section.

## III. EQUIVALENT SYSTEM MODEL

We define

$$(\mathbf{I} + \mathbf{H}_{bj}\mathbf{Q}_j\mathbf{H}_{bj}^H)^{-1} = \mathbf{C}\mathbf{C}^H \quad (7)$$

for its positive semi-definition. According to the Sylvester's determinant theorem, that is,  $\det(\mathbf{I}_m + \mathbf{A}\mathbf{B}) = \det(\mathbf{I}_n + \mathbf{B}\mathbf{A})$ , for any  $\mathbf{A} \in \mathbb{C}^{m \times n}$  and  $\mathbf{B} \in \mathbb{C}^{n \times m}$ ,  $R_b$  can thus be simplified as

$$R_b = \ln \left| \mathbf{I} + \tilde{\mathbf{H}}_{ba}\mathbf{Q}_a\tilde{\mathbf{H}}_{ba}^H \right| \quad (8)$$

where  $\tilde{\mathbf{H}}_{ba} \triangleq \mathbf{C}^H\mathbf{H}_{ba}$  is defined as the equivalent channel matrix.

In doing this way, the four-node wiretap channel with a jammer has been transformed into the conventional three-node wiretap channel, which is depicted in Fig. 2. The equivalent received signals at Bob and Eve are given in (9).

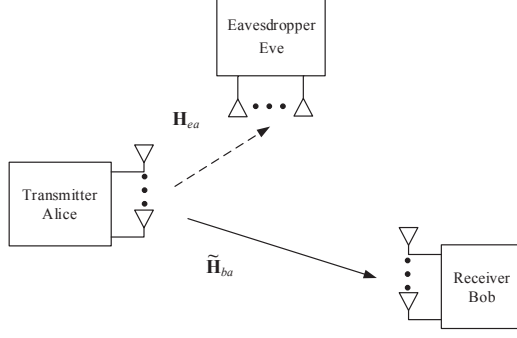


Fig. 2. The equivalent MIMO wiretap channel

$$\begin{aligned}\tilde{\mathbf{y}}_b &= \tilde{\mathbf{H}}_{ba} \mathbf{x}_a + \tilde{\mathbf{n}}_b \\ \mathbf{y}_e &= \mathbf{H}_{ea} \mathbf{x}_a + \mathbf{n}_e\end{aligned}\quad (9)$$

In (9),  $\tilde{\mathbf{y}}_b \triangleq \mathbf{C}^H \mathbf{y}_b$  and  $\tilde{\mathbf{n}}_b \triangleq \mathbf{C}^H (\mathbf{H}_{bj} \mathbf{j} + \mathbf{n}_b)$  are defined as the equivalent received signal and white noise at Bob,  $\tilde{\mathbf{n}}_b \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ .

#### IV. TRANSMIT DESIGN WITH DIFFERENT LEVELS OF ECSI

##### A. Unknown ECSI at Alice

In many applications, it is impractical to assume that full ECSI is available to Alice. When the ECSI is unknown to Alice, it is infeasible to solve the problem in (4) directly. In [14], it has been indicated that maximizing the AN can improve the secrecy performance as long as a desired SINR is guaranteed to achieve. However, the scheme proposed in [14] merely aims at single-flow data transmission, that is, only one spatial dimension is exploited for information symbols while the others are exploited for AN. In fact, we are able to degrade Eve's reception subspace with only  $N_E$  spatial dimensions being allocated to AN. Therefore, in this subsection, we put forward another algorithm which makes effective use of spatial dimension to further improve the secrecy performance. To be specific, we first specify a target data rate  $R$  for Bob. Then  $N_e$  dimensions are allocated to AN which is generated to be orthogonal with the information symbols at Bob. Next, a proper scheme is designed to achieve the target data rate with the smallest possible power allocated to the information symbols. Particularly, it should be mentioned that some target rate may be unreachable in some cases, in such cases, the communication is assumed to be in outage. Apparently, the more power allocated to AN, the more degradation Eve will encounter. But one can notice that the secrecy rate will also decrease resulted from less power allocated to information symbols. Hence, the power distribution ratio between information and AN, denoted by  $\rho$ , should be determined prudently.

With AN being transmitted, the transmit signal  $\mathbf{x}_a$  can be decomposed into the following form,

$$\mathbf{x}_a = \mathbf{W}_u \mathbf{u} + \mathbf{W}_z \mathbf{z} \quad (10)$$

where  $\mathbf{u} \in \mathbb{C}^{d_1}$  is information-bearing signal intended for Bob,  $\mathbf{z} \in \mathbb{C}^{d_2}$  is the AN created by Alice. The elements of  $\mathbf{z}$  are chosen to be i.i.d. complex Gaussian random variables. Assume that  $\mathbf{u} \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_u)$  and  $\mathbf{z} \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_z)$ ,  $\mathbf{u}$  and  $\mathbf{z}$  are assumed to be independent.  $\mathbf{W}_u \in \mathbb{C}^{N_A \times d_1}$  and  $\mathbf{W}_z \in \mathbb{C}^{N_A \times d_2}$  represent the precoding matrix and the AN shaping matrix respectively, in which  $d_1$  and  $d_2$  represent the spatial dimension allocated for  $\mathbf{u}$  and  $\mathbf{z}$ . To avoid the AN interference at Bob,  $(\mathbf{W}_u, \mathbf{W}_z)$  should be an orthogonal basis of  $\mathbb{C}^{N_A}$ .

We consider the total power budget denoted by  $P$ , and then we arrive at

$$\begin{aligned}\mathbf{Q}_u &= \text{diag}(P_1, P_2, \dots, P_{d_1}), \text{Tr}(\mathbf{Q}_u) = \rho P \\ \mathbf{Q}_z &= \frac{(1-\rho)P}{d_2} \mathbf{I}, \text{Tr}(\mathbf{Q}_z) = (1-\rho)P\end{aligned}\quad (11)$$

where  $P_i (i = 1, 2, \dots, d_1)$  denotes the power allocated to  $i$ th information symbol. Note that the AN power is uniformly distributed to each AN symbol, which has been proved to be the best option for Alice in [15].

Since the ECSI is unknown, Alice is assumed to begin with  $N_E$  spatial dimension being allocated to AN to degrade Eve's reception. Meanwhile, more dimensions will be allocated to information symbols if the target rate is too high to achieve. As a result, if  $c$  is assumed to be the number of nonzero singular value of  $\tilde{\mathbf{H}}_{ba}$ , Alice should choose  $\mathbf{W}_u$  as the right singular vectors corresponding to the  $\min(N_A - N_E, c)$  largest singular values of  $\tilde{\mathbf{H}}_{ba}$ . Here, we suppose that Alice is equipped with more antennas than Eve, i.e.,  $N_A > N_E$ .  $\mathbf{W}_z$  must be composed of the remaining  $N_A - d_1$  right singular vectors of  $\tilde{\mathbf{H}}_{ba}$ . Hence, we have

$$\begin{aligned}d_1 &= \min(N_A - N_E, c) \\ d_2 &= N_A - d_1\end{aligned}\quad (12)$$

Then the real data rate for Bob is given by

$$R_b = \sum_{i=1}^{d_1} \ln(1 + \sigma_i^2 P_i) \quad (13)$$

where  $\{\sigma_i\}_{i=1}^{d_1}$  are the  $d_1$  largest nonzero singular values of  $\tilde{\mathbf{H}}_{ba}$ .

To minimize the fraction of the transmit power required to achieve the target rate  $R$ , a power allocation minimum design can be formulated as

$$\begin{aligned}& \min_{P_i, i=1, \dots, d_1} \sum_{i=1}^{d_1} P_i \\ & \text{s.t.} \quad \sum_{i=1}^{d_1} \ln(1 + \sigma_i^2 P_i) = R \\ & \quad \mathbf{p} \triangleq [P_1, P_2, \dots, P_{d_1}]^T \succeq \mathbf{0} \\ & \quad \sum_{i=1}^{d_1} P_i \leq P\end{aligned}\quad (14)$$

Recalling the conventional water-filling algorithm, one can find that (14) operates in an inverse way. Hence, we name our algorithm as an inverse water-filling algorithm.

Let  $P_i = \frac{e^{x_i}-1}{\sigma_i^2}$ , for  $i = 1, \dots, d_1$ . Problem (14) can be equivalently expressed as

$$\begin{aligned} \min_{x_i, i=1, \dots, d_1} \quad & \sum_{i=1}^{d_1} \frac{e^{x_i}}{\sigma_i^2} \\ \text{s.t.} \quad & \sum_{i=1}^{d_1} x_i = R \\ & -\mathbf{x} \triangleq -[x_1, x_2, \dots, x_{d_1}]^T \preceq \mathbf{0} \\ & \sum_{i=1}^{d_1} \frac{e^{x_i}}{\sigma_i^2} \leq P + \sum_{i=1}^{d_1} \frac{1}{\sigma_i^2} \end{aligned} \quad (15)$$

It's easy to verify that the power allocation minimum problem above is convex with respect to  $\{x_i\}_{i=1}^{d_1}$ .

However, an intractable problem the power allocation minimum design may incur is that, the target rate could be unreachable under the total power constraint. To tackle it, let us consider a relaxed power allocation minimum problem where the total power constraint is dropped. By doing so, if the solution of the relaxed power allocation minimum problem does not satisfy the total power constraint, then more dimensions will be allocated to the information signal. Particularly, if the target rate is still unreachable when all the power has been allocated to the information signal, we will break off the link directly.

To solve the relaxed power allocation minimum problem, we consider the following Lagrangian of it,

$$L(\mathbf{x}, \lambda, \nu) = \sum_{i=1}^{d_1} \frac{e^{x_i}}{\sigma_i^2} - \lambda^T \mathbf{x} + \nu \left( \sum_{i=1}^{d_1} x_i - R \right) \quad (16)$$

where  $\lambda$  and  $\nu$  are the Lagrange multipliers associated with the constraint  $\mathbf{x} \succeq \mathbf{0}$  and  $\sum_{i=1}^{d_1} x_i = R$ , respectively. By Slater's condition [16], the strong duality holds true for the **relaxed** power allocation minimum problem. Then the optimal  $\mathbf{x}$  can be obtained from the KKT conditions as below.

$$\frac{\partial \sum_{i=1}^{d_1} \frac{e^{x_i}}{\sigma_i^2}}{\partial x_i} - \frac{\partial \lambda^T \mathbf{x}}{\partial x_i} + \frac{\partial v \left( \sum_{i=1}^{d_1} x_i - R \right)}{\partial x_i} = 0 \quad (17)$$

$$\sum_{i=1}^{d_1} x_i - R = 0 \quad (18)$$

$$\lambda_i \geq 0 \quad (19)$$

$$-\lambda_i x_i = 0 \quad (20)$$

which yields

$$\frac{e^{x_i}}{\sigma_i^2} + v = \lambda_i \quad (21)$$

By (18)-(21), we consider the following two cases to solve the optimal  $P_i$ .

- $\lambda_i > 0$  and  $x_i = 0 \Rightarrow \lambda_i = \frac{1}{\sigma_i^2} + v > 0 \Rightarrow \ln(-v\sigma_i^2) < 0$
- $\lambda_i = 0$  and  $x_i \geq 0 \Rightarrow x_i = \ln(-v\sigma_i^2) \geq 0$

It can be extracted from the two above cases that

$$x_i^{opt} = \max(0, \ln(-v\sigma_i^2)) \Rightarrow P_i^{opt} = \max(0, -v - \frac{1}{\sigma_i^2}) \quad (22)$$

The optimal  $\nu$  can be solved from (18) in the similar way as conventional water-filling algorithm. The overall procedures proposed for the unknown ECSI case have been summarized in **Algorithm 1**.

---

**Algorithm 1** The optimal strategy for Alice without ECSI

---

- 1: Initialize the target data rate  $R$ , the number of Eve's antennas  $N_E$ , the total power budget  $P$ .
  - 2: Compute the singular value decomposition of  $\tilde{\mathbf{H}}_{ba}$ .
  - 3: Compute  $d_1 = \min(N_A - N_E, c)$ ,  $d_2 = N_A - d_1$ , then determine  $\mathbf{W}_u, \mathbf{W}_z$  according to the tactics above (12).
  - 4: Obtain  $P_i^{opt}$  and  $\rho$  by  $P_i^{opt} = \max(0, -v - \frac{1}{\sigma_i^2})$  and  $\rho = (\sum_{i=1}^{d_1} P_i)/P$ , respectively.
  - 5: **while**  $\rho > 1$
  - 6:  $d_1 = d_1 + 1, d_2 = d_2 - 1$ , renew  $\mathbf{W}_u$  and  $\mathbf{W}_z$  by the tactics above (12).
  - 7: Recompute  $P_i^{opt}$  and  $\rho$ .
  - 8: **end while**
  - 9: **if**  $\rho > 1$
  - 10: Break off the link, and  $R_b = 0$ .
  - 11: **else**
  - 12: Output  $P_i^{opt}, \rho$ .
  - 13: **end if**
- 

In particular, it should be reminded that for the case of unknown  $N_e$ , one can start by initializing  $d_1 = 1$ . The secrecy rate obtained from **Algorithm 1** is given by

$$R_s = \begin{cases} R - \ln |\mathbf{I} + \Phi| & \text{if } R \text{ is achievable} \\ 0 & \text{otherwise} \end{cases} \quad (23)$$

where  $\Phi = (\mathbf{I} + \mathbf{H}_{ea} \mathbf{W} \mathbf{Q}_z \mathbf{W}^H \mathbf{H}_{ea}^H)^{-1} \mathbf{H}_{ea} \mathbf{V} \mathbf{Q}_u \mathbf{V}^H \mathbf{H}_{ea}^H$ , in which  $\mathbf{Q}_z$  and  $\mathbf{Q}_u$  are given by (11), and  $\mathbf{Q}_u$ 's diagonal elements are composed of  $\{P_i^{opt}\}_{i=1}^{d_1}$ .

### B. Statistical ECSI at Alice

When only the statistical ECSI is available to Alice, a general approach is to consider the ergodic secrecy rate maximization (ESRM) problem. However, the problem of ESRM is challenging for the barriers of solving the optimization problem. Alternatively, one can choose to concentrate on maximizing the lower bound of ergodic secrecy rate. In [11], this problem has been derived by *Yan Zhu et.al.* However, the iterative algorithm proposed in [11] are unpractical and inefficient for its high complexity to compute the lower bound. Instead, in this subsection, we put forward an alternative solution to tackle the case of statistical ECSI.

Consider that Alice has an access to the statistical ECSI, we employed a stochastic simulation method. Specifically, some simulated channel between Alice and Eve can be randomly generated based on the distribution of  $\mathbf{H}_{ea}$ . The key idea

is that, from the characteristics of Gaussian distribution, the simulated channels will assemble in a restricted interval with high probability. Hence, the estimation error will also be restricted in an acceptable scope. And then, the ergodic secrecy capacity can be approximated as the average secrecy capacity of the simulated channels. To this end, a great number of simulated channels are expected to generate to reduce the average error. According to our later numerical results, we can attain a secrecy performance identical to [11] within five channel trials.

AN is assumed to be transmitted to degrade Eve's reception. We number the simulated channels as  $\hat{\mathbf{H}}_{ea}(i)$ ,  $i = 1, 2, \dots, N_{sim}$ ,  $N_{sim}$  denotes the total number of simulated channels. Similarly to the tactics for unknown ECSI, the precoding matrix  $\mathbf{W}_u$  is assumed to be composed of the right singular vectors corresponding to the  $r$  largest singular values of  $\tilde{\mathbf{H}}_{ba}$ . The AN shaping matrix  $\mathbf{W}_z$  is composed of the remaining  $N_A - r$  right singular vectors of  $\tilde{\mathbf{H}}_{ba}$ . We suppose the power distribution ratio between information and AN is denoted as  $\rho$  yet. Then the secrecy rate for  $i$ th simulated channel is given by ( $i = 1, 2, \dots, N_{sim}$ )

$$\hat{R}_s(r, \rho, i) = \ln |\mathbf{I} + \mathbf{H}_{ba} \mathbf{V} \mathbf{Q}_u \mathbf{V}^H \mathbf{H}_{ba}^H| - \ln |\mathbf{I} + \hat{\Phi}(i)| \quad (24)$$

where

$$\hat{\Phi}(i) = (\mathbf{I} + \mathbf{H}_{ea} \mathbf{W} \mathbf{Q}_z \mathbf{W}^H \mathbf{H}_{ea}^H)^{-1} \hat{\mathbf{H}}_{ea}(i) \mathbf{V} \mathbf{Q}_u \mathbf{V}^H \hat{\mathbf{H}}_{ea}^H(i),$$

and  $\mathbf{Q}_u$  and  $\mathbf{Q}_z$  can be expressed by

$$\mathbf{Q}_u = \rho P \cdot \text{waterfilling}(\rho, r), \mathbf{Q}_z = \frac{(1 - \rho)P}{N_A - r} \mathbf{I} \quad (25)$$

in which the optimal power allocation matrix for the information symbols is obtained via the water-filling algorithm. The global suboptimal  $\rho^*$  and  $r^*$  are thereby attained by maximizing the average secrecy capacity of the simulated channels. The overall procedures for the statistical ECSI case have been summarized in **Algorithm 2**.

The search for  $\rho^*$  can be implemented by adopting the one dimension search algorithms, such as, golden section search and bisection search. The search for  $r^*$  can be simply completed via exhaustive search method. The later numerical results in section V indicate that the total complexity of the above procedures is much less than that in [11].

### C. Full ECSI at Alice

When Alice gets an access to full ECSI, the SRM design is reformulated as

$$\begin{aligned} R_s^* &= \max \ln |\mathbf{I} + \tilde{\mathbf{H}}_{ba} \mathbf{Q}_a \tilde{\mathbf{H}}_{ba}^H| - \ln |\mathbf{I} + \mathbf{H}_{ea} \mathbf{Q}_a \mathbf{H}_{ea}^H| \\ \text{s.t. } &\text{Tr}(\mathbf{Q}_a) \leq P \end{aligned} \quad (26)$$

To solve (26), the AO algorithm proposed by *Qiang Li* in [5] is utilized in our paper. Alternatively, one can adopt the GSVD algorithm proposed in [6] to deal with (26). The results of AO algorithm and GSVD algorithm will be presented in section V.

---

### Algorithm 2 The optimal strategy for Alice with statistical ECSI

---

- 1: Initialize the number of Eve's antennas  $N_E$ , the total power budget  $P$ , the simulation number  $N_{sim}$ , the number of nonzero singular value of  $\tilde{\mathbf{H}}_{ba}$   $c$ .
  - 2: Generate  $N_{sim}$  simulated channel matrices according to the distribution of  $\mathbf{H}_{ea}$ .
  - 3:  $\rho^* = \arg \max_{\rho \in [0,1]} \left( \sum_{i=1}^{N_{sim}} \max_{r \in \mathbb{Z}_+, 1 \leq r \leq c} \hat{R}_s(r, \rho, i) \right)$ .
  - 4:  $r^* = \arg \max_{r \in \mathbb{Z}_+, 1 \leq r \leq c} \left( \sum_{i=1}^{N_{sim}} \hat{R}_s(r, \rho^*, i) \right)$ .
  - 5: Compute the optimal power allocation matrix  $\mathbf{p}$ ,  $\mathbf{p}^* = \text{waterfilling}(\rho^*, r^*)$
  - 6: Choose  $\mathbf{W}_u$  as the right singular vectors corresponding to the  $r^*$  largest singular values of  $\tilde{\mathbf{H}}_{ba}$ . Choose  $\mathbf{W}_z$  as the remaining  $N_A - r^*$  right singular vectors of  $\tilde{\mathbf{H}}_{ba}$
- 

## V. NUMERICAL RESULTS

In this section, we illustrate some numerical results to evaluate the performance gains of our proposed approaches. The parameters are set as:  $N_A = 6$ ,  $N_E = N_J = N_B = 4$ , the total power budget  $P = 10$  dB. All channels follow an i.i.d. complex Gaussian distribution with zero mean and unit variance.

Fig. 3 shows the performance of various algorithms designed for different levels of ECSI. We can see that better performance is always achievable with more ECSI. Particularly, the AO algorithm achieves the best performance among these algorithms. For the case of unknown ECSI, as seen, the average secrecy rate decreases significantly with the increment of jamming power. In addition, a lower target rate,  $R = 4$  bps/Hz, performs better than a higher target rate  $R = 8$  bps/Hz in high jamming power region. Namely, higher target rate means higher outage probability, thus leading to worse performance. As  $R$  increases to 12 bps/Hz, the outage happens when the jamming power is only 6 dB. For the case of statistical ECSI, we compare the performance of our stochastic simulation method with the iterative method proposed in [11]. We can find that our stochastic method even outperforms the iterative method in low jamming power region, also performs identically to the iterative method in high jamming power region. As for the reason, the iterative method only aims at maximizing the lower bound of the ergodic secrecy capacity while the stochastic method aims at maximizing an approximate ergodic secrecy capacity. Though the stochastic method requires myriads of simulated channels, the complexity is still much less than the iterative method, as shown in Fig. 4.

In Fig. 4, the runtime of stochastic search method can be 14 dB less than that of iterative algorithm in average. The notable runtime gap demonstrates the computational efficiency of stochastic search method. However, one can foresee that the stochastic method may be impractical when the scale of system keeps expanding, such as, in the massive MIMO system.

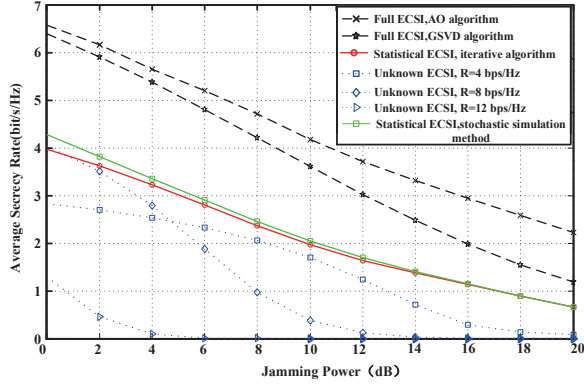


Fig. 3. Average secrecy rate versus the jamming power in various cases

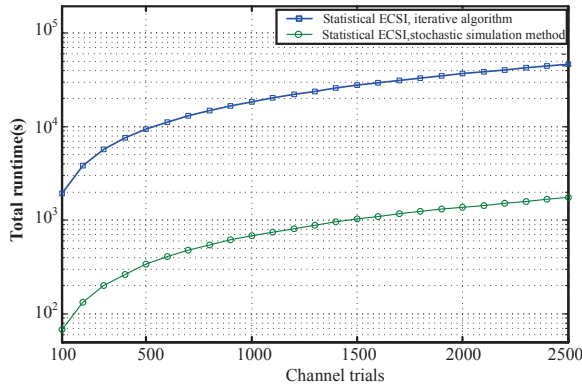


Fig. 4. Total runtime comparison between two methods in the case of statistical ECSI

## VI. CONCLUSION

In this paper, we have studied a four-node wiretap channel with a malicious jammer. The system model is transformed into the transmitter-receiver-eavesdropper wiretap channel by whitening the interference at the legitimate receiver. With various levels of ECSI available to the transmitter, that is, full ECSI, unknown ECSI, and statistical ECSI, different transmission strategies are put forward to improve the secrecy performance. When no ECSI is available, we set a target rate for the legitimate receiver, and determine the power allocation matrix for information symbols by an inverse water-filling algorithm. A high target rate may encounter high outage probability, so the setting of target rate has to be prudent. When statistical ECSI is available, a stochastic simulation method is adopted to avoid the high complexity of iterative algorithm proposed in [11]. It can be seen that the stochastic simulation method can yield the performance identical to the iterative algorithm along with higher computational efficiency. Finally, when full ECSI is available, AO algorithm and GSVD algorithm, designed for conventional wiretap channel, are modified to solve the SRM problem in our paper.

## REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [2] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*. Springer Publishing Company, Incorporated, 2013.
- [3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
- [4] —, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
- [5] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.
- [6] S. A. A. Fakoorian and A. L. Swindlehurst, "Optimal power allocation for gsvd-based beamforming in the MIMO gaussian wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2012)*, Cambridge, MA, Jul. 2012, pp. 2321–2325.
- [7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
- [8] J. Li and A. P. Petropulu, "On ergodic secrecy rate for gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.
- [9] J. Li and A. P. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with rician fading," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 861–867, Sep. 2011.
- [10] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
- [11] Y. Zhu, Y. Zhou, S. Patel, X. Chen, L. Pang, and Z. Xue, "Artificial noise generated in MIMO scenario: optimal power design," *IEEE Signal Process. Lett.*, vol. 20, no. 10, pp. 964–967, Oct. 2013.
- [12] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.
- [13] A. Bayesteh, M. Ansari, and A. Khandani, "Effect of jamming on the capacity of MIMO channels," in *Proc. 42nd Annu. Allerton Conf. Communications, Control and Computing*, Monticello, IL, Oct. 2004, pp. 401–410.
- [14] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
- [15] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.
- [16] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2009.